UNITED STATES DEPARTMENT OF ENERGY (US DOE)
PRIVACY VOLUNTARY CODE OF CONDUCT (VCC)

MISSION STATEMENT

The purpose of the United States Department of Energy Federal Smart Grid Task Force Voluntary Code of Conduct is to describe principles for voluntary adoption that:

(1) encourage innovation while appropriately protecting the privacy of Customer Data and providing reliable, affordable electric and energy-related services;

(2) provide customers with appropriate access to their own Customer Data; and

(3) do not infringe on or supersede any law, regulation, or governance by any applicable federal, state, or local regulatory authority.

The VCC's recommendations are intended to apply as high level principles of conduct for both utilities and third parties.

The VCC is intended to be applicable to, and voluntarily adopted by, both utilities and third parties. However, it is envisioned that the VCC could be most beneficial to either entities that are not subject to regulation by applicable regulatory authorities, or entities whose applicable regulatory authorities have not imposed relevant requirements or guidelines.

The intent is for utilities and third parties to consider adopting the VCC in its entirety. However, a utility or third party could potentially adopt the principles of the VCC with some limited exception, such as when laws, regulatory guidance, governing documents, and/or prevailing state/local business practices indicate a different approach. In these instances, utilities or third parties should explicitly note the reason for the deviation(s) and prominently indicate such in any depiction that they have adopted the VCC, such as in a privacy policy or other notice of adoption. Nothing in this VCC is intended to change, modify, or supersede state/local laws or regulatory guidance.

NOTICE & AWARENESS

Requirements related to communicating applicable policies, and related choices, to customers.

1. **Principle of Data Management**
    - *Collection*
        - Companies should notify customers of the types of information that are being collected.
        - Companies should notify customers, at a high level and easy to understand language, how their data is being collected.
    - *Use*
        - Companies should inform customers why the information is being collected (e.g. billing, rate structures, federal/state programs, customer communications, and for other purposes outside the normal course of business).
        - Companies should provide an overview of what the data will not be used for (if applicable).
        - Companies should explain how individual level data will be used, including when it is used.
        - Companies should explain that data they collect may be used in conjunction with or merged with other data.
    - *Security*
        - Companies should inform customer of high-level methods for securing data throughout the lifecycle of the data and that their data is secured in accordance with any requirements of applicable regulatory authorities.
    - *Sharing*
        - Companies should generally notify customers of all parties with whom data is being shared with (service providers, contractors, etc.).
        - Companies should inform customers of the company's duty to respond to certain legal and regulatory requests.
        - Companies should inform customers of the purpose of sharing the data.
    - *Retention & Disposal*
        - Customers should be informed that CEUD will be retained and disposed of consistent with applicable local, state, and federal record retention rules and regulations, as well as company policies.
        - Companies should include a statement regarding the conversion of some data from hard copy to soft/electronic copy.

2. **Principle of Notification**
    - Companies should provide notice to customers in generally acceptable formats (i.e. paper and/or electronic) as appropriate and as may be required by applicable regulatory authorities.

NOTICE & AWARENESS – CONT'D

- Companies should provide to customers, at minimum, notice at the initiation of service and annually thereafter.
- Companies should make customer notices available online and by customer request.
- Companies should provide materials in various formats that are easily understandable by the demographics they serve.
- Customers should be provided with an updated notification when there is a substantial change in procedure or ownership that would have impact on customer data.
- Notice should include, at minimum:
  - An effective date
  - A point of company contact
  - If notifying of a change in policy, a summary of the changes, or a means by which prior versions can be obtained
  - Protections against unauthorized access
- Notice should be reviewed at least annually and to meet current regulatory/legal requirements.

3. **Principle of Customer Rights**
   - *Rights of Awareness*
     - Customer should be given notice that they have the right to ask the company what data is collected, what it is used for, and who has access to it.
     - Customer should be given notice that their information may be shared to fulfill a Primary Purpose.
     - Customer should be notified of their right to consent to the sharing of their data for secondary purposes as outlined in the Principles of Choice & Consent.
   - *Rights of Access*
     - The notice should inform the customer of their rights to access, review, and dispute the applicable data.
   - *Rights of Dispute Resolution*
     - Customer should be notified of their ability to dispute errors and potentially correct those errors in their applicable data.
     - Customer should be notified of the company's dispute process, including possible recourses for disputing a company's decision.
4. **Principle of Data Classification**
   - *Energy Usage Data*
     - Notice should identify source of information (i.e., meters, credit reports, etc.).

NOTICE & AWARENESS – CONT'D

- *Personally Identifiable Information –*
- Notice should identify source of information (i.e., online, consumer hotline, mail, consumer credit report, etc.).

  Shared Data
  - Notice should state the conditions under which data may be shared.
  - Notice should explain how company may obtain and/or share information from other sources, as well (i.e., credit reporting agency or government entity, contracted agents).
  - Customers should be told what sharing they can opt in to accept and how to do it.
- *Aggregated Data*
  - Inform customers that Aggregated Data may be used and shared to fulfill certain business purposes.

5. **Principle of Customer Awareness**
   - *Data Collection*
     - Companies should be able to educate customers about any questions they have regarding the reasons for data collection.
   - *Privacy Rights*
     - Company should inform the customer, broadly, of their privacy rights.
     - Company should inform the customer of ways to access privacy policies, rules, and/or notices.
   - *Customer Responsibility*
     - Customer should be educated on what their responsibilities as a customer entails (e.g., providing accurate data, notifying company of changes to data, etc.).

CHOICE AND CONSENT

Policy principles related to the customer's granting of authorization for the release/sharing of his or her data.

1. Principle of Customer Control

- Electricity distribution companies require access to customer energy usage data as a condition of service.
- Customers should have access to their own energy usage data.
- Customers should have the ability to share, or not to share, their energy usage data with third parties.
- Customers should have the ability to authorize differential disclosures of their energy usage data among multiple third parties.
- Customers should have the ability to rescind disclosure authority previously granted to a specific third party in a manner that is convenient and easily understood.

2. Principle of Informed Consent

- The processes by which customers exercise informed consent should be convenient, accessible, and easily understood.
- Customers should base consent decisions on an understanding of specifically which of their energy use data is proposed to be shared with a given party, for what purpose, and for how long.
- Customers should base consent decisions on an understanding of all disclosure-related choices available to them.
- Customer consent should be specifically and affirmatively expressed.

3. Principle of Valid Consent

- The processes by which customers exercise informed consent should be secure so that customers are protected against disclosures based on fraudulent consent.
- To the extent a process is needed to ensure the validity of customer authorizations (on-line processes may be secure without additional validation), privacy policies should clearly define the party responsible for conducting such validations.

4. Principle of Controlled Disclosure

- Disclosure should be limited to that energy usage data which the customer has authorized for a specific party for a specific purpose. Authorized parties can disclose CEUD to their Agents.
- Any party that discloses CEUD should retain, or cause to be retained, a record of disclosures so that customers can identify all the parties receiving their energy usage

information, and ascertain that disclosures were given consistent with regulatory requirements or industry standards, as appropriate.

- A duly authorized disclosure should cease when (a) the customer rescinds his or her authorization, (b) the authorization expires, or (c) the customer terminates electric service.
- When an entity receiving duly authorized CEUD is sold, the party providing the CEUD is not required to notify the customer of the change in ownership, and the new owner can continue receiving CEUD without the need for a new disclosure authorization. However, the entity receiving CEUD must notify the customer of the change in ownership.

5. Principle of Efficient Management

- The business processes supporting consumer choice and consent should be cost efficient, and utilize standard formats.

SELF ENFORCEMENT MANAGEMENT AND REDRESS

1. Company Management and Customer Redress

a. The organization will regularly review its information practices for process improvement opportunities and compliance.

b. The organization will take action to meet legal mandates and ensure when necessary appropriate privacy practices.

c. The organization will provide a simple, efficient, and effective means for addressing individual customer concerns. This process will be easily accessible to the customers and provide timely review, investigation, documentation, and, resolution of the customer's concern.

d. On all issues above, the organization will follow existing procedures established or approved by the Applicable Regulatory Authority or Governing Documents, if any. Meeting such applicable procedures will be sufficient to demonstrate compliance with, or under, the VCC.

DATA ACCESS AND PARTICIPATION

Data Collection		Workgroup Consensus	Workgroup Majority
1	*Reasons for Customer Data Collection*	X	

Customer Data is collected to support Primary Purposes, or with the customer's consent to support Secondary Purposes.

References	Workgroup Notes
• U.S Department of Energy, Data Access and Privacy Issues of Smart Grid Technologies (Oct.5, 2010) • NISTIR 7628, Vol. 2 • NAESB REQ.22.3.4 • California Civil Code 1798.98(b) • 4 Code of Colorado Regulations (CCR) 723-3, part 3026(a) • California PU Code 8380 (e)(2); CPUC Decision D.11-07-056; CPUC Decision D.12-08-045	**[Question to DOE Workgroups**: Do we need a reference here to customer notice about data collection practices?]

Data Collection		Workgroup Consensus	Workgroup Majority
2	*Data Minimization*	X	

Service providers should only collect Customer Data that is necessary to accomplish a Primary Purpose, or with consent to support a Secondary Purpose.

References	Workgroup Notes
• White House (February 2012). Consumer Data Privacy In a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. (Consumer Privacy Bill of Rights) • NISTIR 7628, Vol. 2 • NAESB REQ.22.3.4 • CPUC Decision D.11-07-056 and CPUC Decision D.12-08-045 • Future of Privacy Forum – Smart Grid Privacy Guidelines for Consumer Energy Data, available at http://www.futureofprivacy.org/wp-content/uploads/FPF_Smart_Grid_Guidelines.pdf	A Primary or Secondary Purpose may include multiple activities. What types of data collection are "necessary" to support a Primary Purpose will vary depending on the type of business doing the data collection and what is understood about the primary purpose at time of collection. If the scope of the Primary Purpose changes over time, adjustments in data collection and retention may be appropriate. The scope of data collection should be identified in the Service Provider's notice to ensure that the Customer is fully informed.

Data Use		Workgroup Consensus	Workgroup Majority
1	*Primary and Secondary Purpose*	X	

Primary Purpose is the use of Account Data or CEUD that is reasonably expected by the customer: (1) to provide service; and (2) including compatible uses in features and services to the customer that do not materially change expectations of customer control and third party data sharing.

Secondary Purpose is the use of Account Data and CEUD that is materially different from the Primary Purpose and is not reasonably expected by the customer relative to the transactions or ongoing services provided to the customer by the Service Provider or their contracted agent.

References	Workgroup Notes
• CPUC Decision D.11-07-056 and CPUC Decision D.12-08-045 • Future of Privacy Forum – Smart Grid Privacy Guidelines for Consumer Energy Data, available at http://www.futureofprivacy.org/wp-content/uploads/FPF_Smart_Grid_Guidelines.pdf • TRUSTed Smart Grid Privacy Program Requirements, available at http://www.truste.com/privacy-program-requirements/TRUSTed-smart-grid/	Primary Use may be at least those uses described in the terms of service governing the service provider's products or the scope of services which give rise to the customer's interaction with the service provider. Where a state jurisdiction has its own definition of "Primary" or "Secondary" purpose, that definition would be used instead. [**Question to DOE Workgroups**: Is this a statement specific to this principle, or do we need something overarching that applies to all VCC principles?]

Data Retention		Workgroup Consensus	Workgroup Majority
1	*Retention Length for Customer Data*	X	

Service providers should retain Customer Data only as long as needed to fulfill the purpose it was collected for, unless they are under a legal obligation to do otherwise.

References	Workgroup Notes
• NISTIR 7628, Vol. 2; NAESB REQ.22.3.5 Use and Retention • NAESB REQ.22.3.5.1.1 • Federal Trade Commission. (March 2012). Protecting Consumer Privacy in an Era of Rapid Change. • California Civil Code 1798.98(f) • CPUC Decision 11-07-056 July 28, 2011and CPUC Decision D.12-08-045 • Colorado Title 700 Subtitle 723-3 • Illinois Title 83: Public Utilities CHAPTER I; SUBCHAPTER c: PART 410; SECTION 410.210 • Ohio – Title 4901:1-10-24	Data disposal or de-identification should occur within a reasonable time after the purpose or legal obligation has expired.

Data Retention		Workgroup Consensus	Workgroup Majority
2	*Customer Data Disposal*	X	

Service providers should securely and irreversibly dispose of or de-identify Customer Data once it is reasonably determined by the Service Provider to be no longer necessary to achieve the purposes for which it was collected, unless they are under a legal obligation to do otherwise.

References	Workgroup Notes
• White House. (February 2012). Consumer Data Privacy In a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. (Consumer Privacy Bill of Rights) • NAESB REQ.22.3.5.1.2 • NISTIR 7628, Vol. 2 • Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule; November 26, 2012; available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf • HIPAA De-Identification Standard §164.514, available at http://www.gpo.gov/fdsys/pkg/CFR-2002-title45-vol1/xml/CFR-2002-title45-vol1-sec164-514.xml • California Civil Code 1798.98(f)	What constitutes "De-identified Customer Data" is further described in the Aggregated Data section, below. The retention period for Customer Data should be identified in the notice provided to customers, and identify whether the customer has a right to request deletion of the data it previously provided. Examples of disposal standards include those identified by NIST (NIST Special Publication 800-88, Guidelines for Media Sanitization, available at: http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf, and Draft Revision, available at: http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf) and the FTC (16 CFR Part 682, available at http://www.ftc.gov/os/2004/11/041118disposalfrn.pdf).

DATA ACCESS AND PARTICIPATION - CONT'D

Data Retention		Workgroup Consensus	Workgroup Majority
3	*Responsibility for Customer Data Previously Shared with Third Parties*	X	

Service providers should maintain records identifying what data has been shared previously with third parties, when the sharing occurred, and with whom the data was shared for as long as the data exists in the service providers' systems or as long as legally required.

References	Workgroup Notes
• NISTIR 7628, Vols. 1 & 2 • NAESB REQ.22.3.1 • 4 Code of Colorado Regulations (CCR) 723-3, part 3030(c)	

Data Access Rights		Workgroup Consensus	Workgroup Majority
1	*Customer Access*	X	

Customers have a right of reasonable access to their own Customer Data.

References	Workgroup Notes
• 45 CFR § 164.524, Access of individuals to protected health information • NISTIR 7628, Vol. 2 • NAESB REQ.22.3.6 • CPUC Decision D.09-12-046; CPUC Decision D.11-07-056; CPUC Decision D.12-08-045 • 4 Code of Colorado Regulations (CCR) 723-3, part 3026(d)	The method of access available to the customer will vary by service provider. The principle does not dictate a particular form or method of access. "Reasonable access" also includes the scope of the customer's request, which must align with the service provider's data collection practices.

Data Access Rights		Workgroup Consensus	Workgroup Majority
2	*Third Party Access to Customer Data With Consent*	X	

Except as specified in Data Access Rights principle 3, customer consent is required before the service provider shall provide a third party with access to that customer's Account Data and CEUD.

References	Workgroup Notes
• U.S Department of Energy, Data Access and Privacy Issues of Smart Grid Technologies (Oct.5, 2010), available at http://energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf • National Institute of Standards & Technology (NIST), U.S. Department of Commerce, March 15, 2013 Draft of Revised Guidelines for Smart Grid Cybersecurity: Vol. 2, Privacy and the Smart Grid, available at http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/DraftNISTIR7628Rev1/nistir-7628_vol2_03-14-2013_draft.pdf • Wisconsin Public Service Commission. (2009). Provision of Energy Utility Customer Information to Focus on Energy. Docket No. 9501-GF-101, available at http://psc.wi.gov/apps35/ERF_view/viewdoc.aspx?docid=115210 • California PU Code 8380(b)(1); D.09-12-046; CPUC Decision D.11-07-056; CPUC Decision D.12-08-045; CPUC Decision D.12-09-025 • California Civil Code 1798.98(b) • 4 Code of Colorado Regulations (CCR) 723-3, part 3026(e) • Future of Privacy Forum – Smart Grid Privacy Guidelines for Consumer Energy Data, available at http://www.futureofprivacy.org/wp-content/uploads/FPF_Smart_Grid_Guidelines.pdf	

DATA ACCESS AND PARTICIPATION - CONT'D

Data Access Rights		Workgroup Consensus	Workgroup Majority
3	*Third Party Access to Customer Data Without Consent*	X	

Prior customer consent is not required to disclose Customer Data in the case of:

(1) third parties responding to emergencies that pose imminent threats to life or property;
(2) law enforcement or other legal officials to whom disclosure is authorized or required by law;
(3) as directed by Federal or State law, or at the direction of appropriate regulatory authority; or
(4) contracted agents of the service provider supporting a Primary Purpose.

References	Workgroup Notes
• U.S Department of Energy, Data Access and Privacy Issues of Smart Grid Technologies (Oct.5, 2010), available at http://energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf • National Institute of Standards & Technology (NIST), U.S. Department of Commerce, March 15, 2013 Draft of Revised Guidelines for Smart Grid Cybersecurity: Vol. 2, Privacy and the Smart Grid, available at http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/DraftNISTIR7628Rev1/nistir-7628_vol2_03-14-2013_draft.pdf • California Civil Code 1798.98(b) • California PU Code 8380(e)(2), (3); CPUC Decision D.11-07-056; CPUC Decision D.12-08-045 • Wisconsin Public Service Commission. (2009). Provision of Energy Utility Customer Information to Focus on Energy. Docket No. 9501-GF-101, available at http://psc.wi.gov/apps35/ERF_view/viewdoc.aspx?docid=115210. • Future of Privacy Forum – Smart Grid Privacy Guidelines for Consumer Energy Data, available at	Consent to data sharing is considered to be implied in instances where the contracted agent has access to Customer Data to support a service provider's Primary Purpose.

	http://www.futureofprivacy.org/wp-content/uploads/FPF_Smart_Grid_Guidelines.pdf		
Data Access Rights		**Workgroup Consensus**	**Workgroup Majority**
4	*Access to Data Other Than Customer Data*	X	

Except as required by law or to support a Primary Purpose, service providers will not share with a third party the customer's: social security number; state or federal issued identification number; financial account number in combination with any security code providing access to the account; Consumer report information provided by Equifax, Experian, TransUnion, Social Intelligence or another consumer reporting agency; individually identifiable biometric data; or first name (or initial) and last name in combination with any one of the following: (1) date of birth; (2) mother's maiden name; (3) digitized or other electronic signature; and (4) DNA profile. Such information should be obtained directly from the Consumer.

References	Workgroup Notes
• HIPAA (45 CFR 164.514(b)(2))	

Data Access Methods		Workgroup Consensus	Workgroup Majority
1	*General*	X	

Methods of providing customer access to Account Data and CEUD should be reasonably convenient, timely, and where appropriate, cost-effective.

References	Workgroup Notes
• 45 CFR § 164.524, Access of individuals to protected health information • CPUC Decision D.09-12-046; and CPUC Decision D.11-07-056; CPUC Decision D.12-08-045 • 4 Code of Colorado Regulations (CCR) 723-3, part 3026(d) & (e)	"Cost effective" is a term commonly used with rate regulated entities to reflect a balance between cost and the value offered to customers. Service Providers that are rate regulated will need to consider cost effectiveness when making decisions about data access methods.

Data Access Methods		Workgroup Consensus	Workgroup Majority
2	*Cost for Customer Data Reports*	X	

To the extent that a service provider offers a method of data access for data requestors that is different from the method it generally offers to its customers, or not based on commonly used data formats or standards, that service provider may charge a fee, subject to applicable laws and regulations.

References	Workgroup Notes
• 4 Code of Colorado Regulations (CCR) 723-3, part 3026(c)(V) • HHS FAQ for establishing costs for the patient data reports • OCR's guidance on "The HIPAA Privacy Rule's Right of Access and Health Information Technology" • FCRA guidance for providing access to financial information/reports/data under the Fair Credit Reporting Act (FCRA), See § 612	Service providers that are rate regulated may have to obtain approval for any fee.

Data Access Methods		Workgroup Consensus	Workgroup Majority
3	*Costs for Aggregated Data Reports*	X	

The service provider may allow for recovery of costs for Aggregated Data requests that is different from the method or format in which it generally offers aggregated data, represents the fulfillment of multiple requests or is not based on commonly used data formats or standards.

References	Workgroup Notes
• California PU Code 394.4(a); California PU Code 8380(e)(1); CPUC Decision D.11-07-056; CPUC Decision D.12-08-045 • 4 Code of Colorado Regulations (CCR) 723-3, part 3031(d)(IV)	Service providers that are rate regulated may have to obtain approval for any fee.

Aggregated Data		Workgroup Consensus	Workgroup Majority
1	*Access to Aggregated Data*	X	

Data that is aggregated in manner that limits the likelihood to re-identify a customer may be made available.

Aggregated Data may be shared via a contract between the service provider and third party that may include language limiting uses of the data, including a requirement to not re-identify customers.

The service provider may decline a request for Aggregated Data release if fulfilling such a release would cause substantial disruption to the day-to-day activities of its personnel.

References	Workgroup Notes
• 4 Code of Colorado Regulations (CCR) 723-3, part 3031 • National Institutes of Health: Health Services Research and the HIPPA Privacy Rule: http://privacyruleandresearch.nih.gov/healthservicesprivacy.asp • CASRO Privacy Policy, Sec.A, 1- 3; http://www.casro.org/?page=TheCASROCode#Confidentiality	Best practices in marketing research and clinical research include contractual agreements between clients and vendors/agencies to limit how the results may be used. Confidentiality of study respondents is to be respected at all times.

DATA ACCESS AND PARTICIPATION - CONT'D

Aggregated Data		Workgroup Consensus	Workgroup Majority
2	*Requirements for Aggregated Data*		
[tabled pending PNNL research]			

References	Workgroup Notes

Aggregated Data		Workgroup Consensus	Workgroup Majority
3	*Aggregated Data Methodologies*	X	

Aggregated Data methodologies should ensure a sufficient number of customers are included in the aggregation to reduce the ability to re-identify a customer.

Methods by which data can be aggregated should be reviewed every 2 years to account for changes in technology.

References	Workgroup Notes
• California PU Code 394.4(a); CPUC Decision D.11-7-056; CPUC Decision D.12-08-045 • California Public Utilities Code Sec. 8380(e)(1), California PUC decision(s) D.11-07-056, D.12-08-045; 45 CFR 164.514(a)-(c) • National Institutes of Health: Health Services Research and the HIPPA Privacy Rule: http://privacyruleandresearch.nih.gov/healthservicesprivacy.asp • CASRO Privacy Policy, Sec.A, 1- 3; http://www.casro.org/?page=TheCASROCode#Confidentiality	Data aggregation is commonplace in other industries but the "how" differs according to industry and intent.

DATA ACCESS AND PARTICIPATION - CONT'D

Aggregated Data		Workgroup Consensus	Workgroup Majority
4	*Exclusions*	X	
Aggregated Data that contains trade secrets, even when aggregated, may not be released.			

References	Workgroup Notes
• National Institutes of Health: Health Services Research and the HIPPA Privacy Rule: http://privacyruleandresearch.nih.gov/healthservicesprivacy.asp • CASRO Privacy Policy, Sec.A, 1- 3; http://www.casro.org/?page=TheCASROCode#Confidentiality	Typically, research organizations allow aggregated data to be released for research purposes; however, energy usage data differs from clinical research or market research, where the data is structured differently and maintains a consistent pattern. Because energy usage patterns may detail a manufacturing process when disaggregated, including patented process improvements, the competition could inadvertently benefit from release of even aggregated data.

INTEGRITY AND SECURITY

Category 1: Security and Safeguards

1. Data Security Methods	
Proposed Principle:	
Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risk to the organization, related entities and customers.	
References	**Examples and Explanatory Implementation Guidance**
• NIST Executive Order Draft Cybersecurity Framework (Oct 2013), *available at:* http://www.nist.gov/itl/upload/discussion-draft_preliminary-cybersecurity-framework-082813.pdf.	o Implement technical, process and administrative controls (including plans and procedures) that are reasonably designed to address existing and foreseeable threats to the confidentiality, integrity, and availability of the operations technology (OT) and information technology (IT) assets, as well as the data which these systems process or store. o Such controls should address both external and internal threats, including employees, vendors and partners. o Responsibility for controls management should extend to the technology, risk, procurement and vendor management; compliance, legal and audit groups with oversight by executive management; and the board of directors, if there is such. o Incorporate data security and privacy protection into contracts or agreements with vendors, partners and other third parties.

INTEGRITY AND SECURITY – CONT'D

2. Data Protection Against Loss, Unauthorized Use, Modification, etc.	
Proposed Principle:	
"**Implement and maintain process, technology, and training measures to ensure data integrity and protect against loss and unauthorized use, access or dissemination**."	
References	**Examples and Explanatory Implementation Guidance**
• NIST Executive Order Draft Cybersecurity Framework (Oct 2013), *available at:* http://www.nist.gov/itl/upload/discussion-draft_preliminary-cybersecurity-framework-082813.pdf.	○ Record and identify access to or movement of CEUD or Account Data consistent with the sensitivity of the data, appropriate business purpose, and technical complexity of the systems. ○ Create and manage identities for entities that may be granted logical or physical access to the organization's assets. ○ Support data integrity and confidentiality through maintenance of a comprehensive record retention program for sensitive or critical data with designated data owners. ○ Implement appropriate technical controls, such as encryption, for data at rest and in transmission. ○ Ensure that all authorized users receive formal training for use and handling of data, and that appropriate administrative measures are instituted for noncompliance.

3. Define Process for Handling Data Breaches	
Proposed Principle:	
Maintain a comprehensive breach response program for the identification, containment, mitigation and resolution of any incident that causes or results in the breach of data security.	
References	**Examples and Explanatory Implementation Guidance**
• NIST Executive Order Draft Cybersecurity Framework (Oct 2013), *available at:* http://www.nist.gov/itl/upload/discussion-draft_preliminary-cybersecurity-framework-082813.pdf.	○ The program should include all relevant internal stakeholders (e.g., technology, security, legal, privacy regulatory relations, corporate communications), as well as a process for involving external entities such as law enforcement agencies and/or incident coordination groups (e.g. ICS-CERT, etc.). ○ It should also include a process for documenting root causes, implementation of remedial measures, and recording lessons learned from the event.

4. Define Process for Customer Notification of Data Breaches	
Proposed Principle:	
Customers should be notified when it is reasonably likely that their personal information has been accessed without authorization under circumstances which may result in misuse of CEUD or Account Data. [Note: Coordinate with Notice/Awareness Group]	
References	**Examples and Explanatory Implementation Guidance**
• NIST Executive Order Draft Cybersecurity Framework (Oct 2013), *available at:* http://www.nist.gov/itl/upload/discussion-draft_preliminary-cybersecurity-framework-082813.pdf.	o Notice should occur within a reasonable period of time after the nature and extent of the breach is determined. o Such notice should inform the customer of the circumstances surrounding the breach, the information about them which may have been affected, what they can or should do to protect themselves against misuse of the information by others, and the steps which have been taken to preclude future, similar events. o The notice should be delivered in a manner consistent with other means by which the customer is advised of significant actions which may affect them, such as changes in policy, delivery of goods or services, or pricing. [Data breach notification: Coordinate with Notice/Awareness group]

5. Define Responsibility for Data Breach Notification and Remedies	
Proposed Principle:	
The Service Provider whose customer's information may have been compromised has the primary responsibility for ensuring the delivery of complete, accurate and timely notice to the customer and remedying the conditions which led to the breach. [Coordinate with Notice/Awareness Group]	
References	**Examples and Explanatory Implementation Guidance**
• NIST Executive Order Draft Cybersecurity Framework (Oct 2013), *available at:* http://www.nist.gov/itl/upload/discussion-draft_preliminary-cybersecurity-framework-082813.pdf.	o "Service Provider" refers to the utility or third party that has adopted the Voluntary Code of Conduct, and whose customer's information may have been compromised, regardless of whether the compromise occurred through the Service Provider itself or through a vendor. o The Service Provider may require, by contract or other agreement, that the entity (e.g., vendor) having actual responsibility for the breach will deliver the notice. However, this must be done in a way that does not confuse the recipient of the notice as to the identity of the Service Provider to whom they originally disclosed the personal information.

Category 2: Data Quality and Accuracy

1. Data Quality	
Proposed Principle:	
Account Data and CEUD should be reasonably accurate and complete, considering the circumstances and environment in which it has been collected (e.g., validated data, data collected indirectly from another entity, etc.). When a Service Provider has modified or enhanced data that it initially received from another source (e.g., a utility or a different third party), the customer receiving the enhanced or modified data should generally be made aware that such data may differ from the initial data.	
References	**Examples and Explanatory Implementation Guidance**
• NAESB REQ 22. North American Energy Standards Board (NAESB), August 8, 2011. http://www.naesb.org/member_login_check.asp?doc=retail_bk22_043012.pdf • NIST Recommended Privacy Practices for Customer/Consumer Smart Grid Energy Usage Data Obtained Directly by Third Parties." Smart Grid Interoperability Panel, Cyber Security Working Group (CSWG), August 13, 2012. http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGPrivacy/Third_Party_Privacy_Best_Practices_Document_v4_Final.pdf • California PUC Rules. Decision Adopting Rules to Protect the Privacy and Security of the Electricity Usage Data of the Customers of Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas and Electric Company." July 28, 2011. http://docs.cpuc.ca.gov/WORD_PDF/FINAL_DECISION/140369.ppd • Vermont Model Privacy Policy: A Model Privacy Policy for Smart Grid Data." Vermont Law School, Institute for Energy and the Environment, accessed January 11, 2013. http://vermontlaw.edu/Documents/Model%20Smart%20Grid%20Privacy%20Policy%20VLS%20Version%202.pdf	○ An authorized third party asks for real-time, 15 minute interval data from a customer's smart meter. Assuming the utility is capable and willing to provide such data, the utility should give the party as reasonably accurate and complete data as is practicable, recognizing that the utility has not had an opportunity to validate the data, and there may be "pings" or "blips" that have not yet been corrected. ○ An authorized fourth party asks for customer data from a third party, who had previously obtained it from a utility. The third party should endeavor to provide as reasonably complete and accurate data as it can, recognizing that the data it provides can only be as accurate and complete as the data it originally obtained. ○ A third party collects customer data from a utility. It then modifies or enhances the data with other information, analysis, etc. If the third party then discloses that data to another party, it should communicate that it has enhanced or modified the data, such that it is different than the data originally received from the utility.

INTEGRITY AND SECURITY – CONT'D

2. Data Accuracy	
Proposed Principle:	
• **Utilities and third parties should provide a process for customers to dispute the accuracy or completeness of their own Account Data or CEUD, and to request appropriate corrections or amendments. Existing procedures for addressing other types of customer complaints may be adequate.** [Note: Coordinate with Management / Redress working group.]	
References	**Examples and Explanatory Implementation Guidance**
• NAESB REQ 22. North American Energy Standards Board (NAESB), August 8, 2011. http://www.naesb.org/member_login_check.asp?doc=retail_bk22_043012.pdf • NIST Recommended Privacy Practices for Customer/Consumer Smart Grid Energy Usage Data Obtained Directly by Third Parties." Smart Grid Interoperability Panel, Cyber Security Working Group (CSWG), August 13, 2012. http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGPrivacy/Third_Party_Privacy_Best_Practices_Document_v4_Final.pdf • California PUC Rules. Decision Adopting Rules to Protect the Privacy and Security of the Electricity Usage Data of the Customers of Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas and Electric Company." July 28, 2011. http://docs.cpuc.ca.gov/WORD_PDF/FINAL_DECISION/140369.pdf • Vermont Model Privacy Policy: A Model Privacy Policy for Smart Grid Data." Vermont Law School, Institute for Energy and the Environment, accessed January 11, 2013. http://vermontlaw.edu/Documents/Model%20Smart%20Grid%20Privacy%20Policy%20VLS%20Version%202.pdf	○ A customer receives a bill from the utility and notices that the bill included the wrong Account Data (email address, account number, rate class, etc.). A process should be available to the customer to contact the utility and correct the mistake. A separate "Customer Data" process may not be necessary if a general customer compliant hotline or other process is sufficient. ○ An authorized third party provides a service to the customer using the customer's Account Data or CEUD as collected from the utility (and possibly enhanced or modified). In reviewing the third party's product, the customer realizes there is a mistake in his or her CEUD or Account Data. The third party should have a process available to the customer to correct the mistake or, if applicable, determine that the mistake was contained in the original data.

Next Steps: Coordinate with other groups after November 22nd face-to-face meeting as noted above in highlighted brackets.

KEY DEFINITIONS

Applicability/Adoption

The VCC is intended to be applicable to, and voluntarily adopted by, both utilities and third parties. However, we envision that the VCC could be most beneficial to either unregulated entities or entities whose applicable regulatory authorities have not imposed relevant requirements or guidelines.

The VCC's recommendations are intended to apply as high level principles of conduct for both utilities and third parties. When drafting the VCC, if a Working Group finds that a distinction needs to be made, it may indicate that they are getting into more detail than desired.

The intent is for utilities and third parties to consider adopting the VCC in its entirety. However, a utility or third party could potentially adopt the principles of the VCC with some limited exception, such as when laws, regulatory guidance, governing documents, and/or prevailing state/local business practices indicate a different approach. In these instances, utilities or third parties should explicitly note the reason for the deviation(s) and prominently indicate such in any depiction that they have adopted the VCC, such as in a privacy policy or other notice of adoption.

Customer Data

Customer Data: the term "Customer Data" refers to the combination of customer energy usage data (CEUD) and Account Data. Customer Data is treated as private and has specific requirements outlined elsewhere in the VCC. CEUD without Account Data is considered anonymous data, which is discussed separately in the VCC, and referred to specifically as "anonymous data." Aggregated CEUD is also discussed separately, and referred to specifically as "aggregated data." Publicly available information about a customer is not treated as private, unless it is combined with other non-public information.

Account Data

Account Data: the following elements, when identified with a specific customer, are considered to be Account Data:

i. Names

ii. All geographic subdivisions smaller than a state, including street address, city, county, precinct, census block, zip code, and their equivalent geo-codes;

iii. Dates of service provided to a customer by the utility or third party or information specific to identifying an individual's utility service;

iv. Telephone or fax numbers;

v. Electronic mail addresses;

vi. Utility or Third Party Account numbers (excluding financial account numbers, such as credit card numbers, bank account numbers, etc.); and

vii. Device identifiers (e.g., meter numbers, HAN numbers, etc.) and serial numbers.

KEY DEFINITIONS – CONT'D

Aggregated data

Aggregated Data is the combination of multiple customer data elements to create a data set that is sufficiently anonymous so that it does not reveal the identity of an individual customer.

Customer Energy Usage Data (CEUD)

Proposed: Customer Energy Usage Data reflects an individual customer's measured energy usage but does not identify the customer.

CHOICE AND CONSENT EXAMPLES

Disclaimer – The following examples are intended to illustrate the principles of customer choice and consent in action. They are not intended to prescribe strategies for implementing customer choice and control. There can be many equally valid ways to do this.

Examples of customer control

The customer wants to authorize a given third party to access his or her energy usage data. The customer is given a series of pre-defined options regarding the kind of data to be disclosed to the third party (e.g., interval, peak load, power quality characteristics), and the duration of the disclosure (e.g., one month, 6 months, 1 year, 3 years, etc.). The customer can specify different authorizations for subsequent third parties, and can subsequently terminate or revoke access for any third party at any time. If the customer has selected a finite authorization period, the customer is notified prior to expiration of that finite period, with an option to renew or terminate continued access by that third party.

Example of informed consent

Before a customer can exercise options for releasing his or her data, he or she must acknowledge that he or she has reviewed the Service Provider's (i.e., third party's or utility's) privacy Terms and Conditions or other privacy notification. (NOTE TO DRAFT – WE NEED A CONSISTENT TERM FOR SERVICE PROVIDERS, ETC. THIS IS SOMETHING THAT SHOULD BE ADDRESSED GLOBALLY, WHEN ALL THE WORK GROUP PRODUCTS ARE INTEGRATED.) These Terms and Conditions and/or other privacy notification describe disclosure-related options available to the customer, and explain that if the customer is asked to authorize access to his or her CEUD, the request will specify the complete nature of the type of data that is proposed to be disclosed to a given party (e.g., interval, peak load, power quality characteristics, Account Data), how the data will be used, and for how long. The Terms and Conditions and/or privacy notification should explain how the customer can access is or her own energy usage data. The documents should also explain how the customer can authorize specific third parties to receive his or her data, and review those authorizations, and how the customer can terminate or modify third party access at any time.

Example of Valid Consent

A third party may obtain access to a customer's data after the customer expressly agrees to allow that access. The method of authorization may vary. The customer may provide that agreement by signing an authorization form or by providing electronic [or recorded] authorization to the third party. Alternatively, the customer may provide non-public account data to gain access to his or her own data directly, or enable a third party to gain such access.

CHOICE AND CONSENT EXAMPLES – CONT'D

Example of Controlled Disclosure

A customer is seeking bids from two service providers for an energy efficiency retrofit project to his or her home. To enable the firms to make effective bids, the customer wants to authorize the firms to access the customer's data for the purpose of designing an optimal application. Having read the Service Provider's privacy Terms and Conditions, or other privacy notification (above), the customer reviews his or her record of authorizations to confirm whether these or any other firms presently are getting the customer's CEUD. Finding none, the customer authorizes both firms to access the customer's CEUD for the most recent 12 months (or whatever time frame option the customer decides is appropriate), and to have this access for one month.

Example of Efficient Management

The customer uses an on-line information system to exercise privacy choices. Once logged in (the customer must provide certain non-public elements of their account data to log in), among the privacy services the customer can obtain are the following three: (1) the customer can view and/or download his or her CEUD, which is provided using a standard data model; (2) the customer can access the utility's privacy policy, and a video clip explaining the customer's privacy-related choices and the implications of each; (3) the customer can authorize third parties to access his or her energy usage data by selecting from a series of drop down menu options that define for the duration of access, and the nature of the data to be provided. The use of an on-line system to provide these services, combined with the use of standard data models and a standard set of customer choices – is significantly more cost-effective than providing the same services manually using custom specifications.